REMARKS

The present Amendment amends claims 23-44. Therefore, the present application has pending claims 23-44.

Claims 23-44 stand objected to due to informalities noted by the Examiner in paragraphs 9-15 of the Office Action. Amendments were made throughout claims 23-44 to correct the informalities noted by the Examiner. Therefore, this objection is overcome and should be withdrawn. Accordingly, reconsideration and withdrawal of this objection is overcome and should be withdrawn.

In paragraphs 18-23, claims 23-44 stand variously rejected under 35 USC §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regards as their invention. Various amendments were made throughout claims 23-44 to bring them into conformity with the requirements of 35 USC §112, second paragraph. Therefore, this rejection with respect to claims 23-44 is overcome and should be withdrawn.

Specifically, amendments were made throughout claims 23-44 to overcome the objections noted by the Examiner in the Office Action.

Claims 23-44 stand rejected under 35 USC §101 as allegedly being directed to statutory subject matter. Amendments were made to the claims so that it is clear that the claims are directed to a practical application, namely the encrypting and decrypting of communications in a computer system which implements a public-key or communication cryptographic method. Thus, the claims now more clearly recite that they are directed to a "process"

implemented by a "machine" as permitted under 35 USC §101. Therefore, reconsideration and withdrawal of this rejection is respectfully requested.

Claims 23-44 stand rejected under 35 USC §103(a) as being unpatentable over Cramer (U.S. Patent No. 6,697,488). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 23-44 are not taught or suggested by Cramer whether taken individually or in combination with any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

As discussed in the REMARKS of the November 17, 2005 Amendment, the contents of which are incorporated herein by reference. As previously discussed the present invention is directed to a public-key cryptographic method implemented in a computer system that generates a secret key and a public key by a key generation step, performs a ciphertext generation and transmission step of selecting random numbers for a plaintext, performs a ciphertext reception and decipher step of calculating from the received ciphertext by using the secret key which satisfies a particular function, performs outputting the deciphered results if the function is satisfied and performs outputting an indication that the received ciphertext is rejected if the function is not satisfied.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly the above described features of the present invention now more clearly recited in the claims are not taught or suggested by Cramer

whether taken individually or in combination with each other or any of the other references of record.

Cramer is directed to a scheme with improve the security of encrypted data or information by using a practical public cryptosystem that is able to resist adaptive attacks. According to Cramer, the scheme does not leak any information of the secret of the used key by generating an extended private key and public key. As per Cramer, a message m, also referred to as plaintext, can be encrypted to obtain a cipher text t by using the public key. This cipher text t can be transmitted over an insecure channel such as the internet so that only a recipient with the right private key is able to decrypt the cipher text t.

The proof of security according to the system taught by Cramer is based on standard assumptions which are the hardness of the Diffie-Hellman decision problem (DDH problem), wherein the DDH problem is very hard to solve due to the large calculation volume; and the collision intractability of the hash function, which is equivalent to the existence of universal one-way functions.

Cramer employs a hash function in the encryption algorithm as described in col. 7, line 50 to col. 8, line 21 and col. 11, line 60 to col. 12, line 34 thereof. Cramer also discloses a particular encryption method using a hash function and the hash value in claims 11 and 12 thereof.

The proof of security of the present invention as described, for example, on page 4, line 26 through page 7, line 4 of the present application relates to a security system which is also based on an assumption of the hardness of the Diffie-Heilman decision problem.

However, the proof security of the present invention is not based on the above described assumption regarding the collision intractability of the hash function through which the existence of the universal one-way functions are provided. In the present invention, a hash function and a hash value are not used in the encryption process.

As is well known, various cryptographic schemes are based on various assumptions. However, such assumptions are not always realistic. The collision intractability of the hash function has not yet been verified. See page 3, line 27 to page 4, line 24 of the present application. Therefore, contrary to Cramer, the present invention does not rely on the unverified assumption of the collision intractability of the hash function for encryption and as such is directed to an encryption process entirely different from Cramer.

Thus, as is quite clear from the above, the present invention is quite different from Cramer, particularly with regard to the assumptions upon. According to the present invention, hash functions and values are not used in the encryption process thereof. Therefore, the features of the present invention as recited in the claims are not taught or suggested by Cramer whether taken individually or in combination with any of the other references of record.

Further, Cramer does not assume the random oracle model but assumes a universal one way hash function contrary to that of the present invention. The universal one way hash function is an algorithm which can prove the security. However, it is an ideal function and it is actually replaced with a practical hash function such as SHA-1. This replacement makes the

proof of the security insecure. This is an inherent problem of Cramer. Attention is directed to the attached article entitled "Random Oracle". This phenomenon is well-known as discussed on page 5, lines 19 and 21 of the present application and as discussed column 5, lines 44 to 47 of Cramer. Cramer refers to this phenomenon as "Collision resistant hash functions"

The present invention does not assume the universal one way hash function and provides an encryption scheme more efficient than Cramer.

In Cramer, the public key includes one element "d" as shown in Fig. 2 and as discussed at column 7, lines 26 to 39 thereof. The element "d" as per Cramer relates to the two elements y1 and y2 of the private key. Cramer does not disclose the detailed structure of the public key. Further, the Examiner does not indicate the relation of each element of the public key between Cramer and the present invention.

In the present invention, the public key includes two elements "d1" and "d2". The "d1" and "d2" of the present invention respectively relate to the two elements y11 and y12, and y21 and y22 of the private key. Independent claims 23, 24, 28 and 30 of the present application each includes "d1" and "d2" in the public key at the key generation step. The ciphertext generating step of the present invention uses the two elements "d1" and "d2" and the ciphertext decipher step of the present invention uses the four elements of y11, y12, y21 and y22 of the private key.

Thus, the present invention as recited in the claims differs substantially for Cramer being that Cramer fails to teach or suggest the

key generation step, ciphertext generation step and ciphertext decipher step as recited in the claims.

Therefore, as is clear from above, the features of the present invention as now more clearly recited in claims 23-44 are not taught or suggested by Cramer. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 23-44 as being unpatentable over Cramer is respectfully requested.

In view of the foregoing amendments and remarks, applicants submit that claims 23-44 are in condition for allowance. Accordingly, early allowance of claims 23-44 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (500.41092X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120

Random oracle

W0012-01EP

From Wikipedia, the free encyclopedia

A **random oracle** is a mathematical abstraction used in cryptographic proofs. Random oracles are typically included in proofs when no "real" function (that can be implemented) provides sufficient mathematical properties to satisfy the proof of security. Proofs which make use of random oracles are referred to as secure in the "random oracle model", as opposed to the "standard model". In practice, random oracles are typically used to model cryptographic hash functions in schemes where strong randomness assumptions are needed of the hash function's output. Such proofs indicate that systems or protocols are secure by showing that an attacker must require impossible behavior from the oracle, or solve some other mathematical problem believed hard, in order to break the protocol. Not all uses of cryptographic hash functions require random oracles: schemes which require only the property of collision resistance can be proven secure in the standard model (e.g., the Cramer-Shoup cryptosystem).

When a random oracle is given a query x it does the following:

- If the oracle has been given the query x before, it responds with the same value it gave the last time.
- If the oracle hasn't been given the query x before, it generates a random response which has uniform probability of being chosen from anywhere in the oracle's output domain.

In the more precise definition formalized by Bellare/Rogaway (1993), the random oracle produces a bit-string of infinite length which can be truncated to the length desired. When a random oracle is used within a security proof, it is made available to all players, including the adversary or adversaries. A single oracle may be treated as multiple oracles by pre-pending a fixed bit-string to the beginning of each query (e.g., queries formatted as "1|x" or "0|x" can be considered as calls to two separate random oracles).

No real function can implement a true random oracle. In fact, certain very artificial protocols have been constructed which are proven secure in the random oracle model, but which are trivially insecure when any real hash function is substituted for the random oracle. Nonetheless, for any more natural protocol a proof of security in the random oracle model gives very strong evidence that an attack which does not break the other assumptions of the proof, if any (such as the hardness of integer factorization) must discover some unknown and undesirable property of the hash function used in the protocol to work. Many schemes have been proven secure in the random oracle model, for example OAEP and PSS.

See also

- Topics in cryptography

References

- Mihir Bellare and Phillip Rogaway, Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, ACM Conference on Computer and Communications Security 1993, pp62–73 (PS and PDF) (http://www.cs.ucsd.edu/users/mihir/papers/ro.html).
- Ran Canetti, Oded Goldreich and Shai Halevi, The Random Oracle Methodology Revisited, STOC 1998, pp209–218 [1] (http://arxiv.org/abs/cs.CR/0010019).

External links

- The Random Oracle Model (http://www.cs.ut.ee/~helger/crypto/link/rom/) - link farm maintained by Helger Lipmaa

Retrieved from "http://en.wikipedia.org/wiki/Random_oracle"